

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,

Plaintiff,

v.

CR 16-4571 JCH

GUY ROSENSCHEIN,

Defendant.

**PROPOSED FINDINGS AND RECOMMENDED DISPOSITION**

This matter comes before the Court on Non-Party Microsoft Corporation's Motion to Modify Rule 17(c) Subpoena [Doc. 125], filed April 18, 2019, and fully briefed on May 20, 2019. [See Doc. 138]. Presiding District Judge Herrera referred the Motion to the undersigned Magistrate Judge for decision pursuant to 28 U.S.C. § 636(b)(1)(A) and Fed. R. Crim. P. 59(a). [See Doc. 139]. The questions presented concern the proper scope and use of a subpoena to a non-party under the Federal Rules of Criminal Procedure. Having considered Defendant Rosenschein's Response to the Motion [Doc. 136], and all pertinent authority, the Court recommends that the Motion be granted. Additionally, the Court recommends that Defendant Rosenschein's Request for Telephonic Hearing on the Motion [Doc. 141], filed May 22, 2019, be denied.

**I. INTRODUCTION**

"It was not intended by [Fed. R. Crim. P.] Rule 16 to give a limited right of discovery, and then by [Fed. R. Crim. P.] Rule 17 to give a right of discovery in the broadest terms." *Bowman Dairy Co. v. United States*, 341 U.S. 214, 220 (1951). For this reason, the materials that can be compelled via a Rule 17(c) subpoena are inherently narrow and specific. *See, e.g., United States v. Nixon*, 418 U.S. 683, 700 (1974). As one court has said, "[t]he relevance and specificity elements

‘require more than the title of a document and conjecture as to its contents,’ and a subpoena should not issue based upon a party’s ‘mere hope’ that it will turn up favorable evidence.” *United States v. Stevenson*, 727 F.3d 926, 831 (8th Cir. 2013) (citation omitted). The proponent of a Rule 17 subpoena may not, therefore, utilize a subpoena to “fish[] for evidence that might support his theory, as if he were in the discovery phase of a civil action.” *United States v. Richardson*, 607 F.3d 357, 368 (4th Cir. 2010).

Defendant Rosenschein’s subpoena to non-party Microsoft in this case contained eighteen (18) separate subparts, requesting, among other things, “[a]ny and all” agreements, guidelines, memorandums of understanding, contracts, correspondence and reports generated by Microsoft in relation to its PhotoDNA Service and its relationships with law enforcement, the National Center for Missing & Exploited Children (NCMEC), and electronic service provider Chatstep. [See Doc. 125-1, pp. 9-12]. Rather than identify specific documents to be produced, Rosenschein’s subpoena reads like a civil discovery request, seeking “the production of essentially any document that would support his theory that [Microsoft] was in an agency relationship with the Government.” See *Richardson*, 607 F.3d at 368. Therefore, because Rosenschein’s subpoena fails to conform to *Nixon*’s specificity requirement, Microsoft’s Motion to Modify the subpoena should be granted. Alternatively, Microsoft’s Motion should be granted because compliance with the subpoena as drafted would be oppressive.

## **II. BACKGROUND**

Rosenschein is charged with the distribution and possession of child pornography. [See Doc. 1]. As stated by Judge Herrera in her most recent Memorandum Opinion and Order, law enforcement began investigating Rosenschein when the Bernalillo County Sheriff’s Office (“BCSO”) received two CyberTipline Reports from the NCMEC. [Doc. 151, p. 2]. The two

CyberTipline Reports that the BCSO received were generated by Chatstep, an electronic service provider that hosts internet-based conversations between users. [*Id.*]. Chatstep was able to identify the alleged child pornography through its use of Microsoft's PhotoDNA service. [*Id.*]. PhotoDNA is a cloud-based service developed by Microsoft to help prevent the sharing of child pornography. [*Id.*]. It works by analyzing digital images to create a unique "hash value" of a file that is then matched against databases of hash values of known child pornography. [*Id.*, pp. 2-3]. Through its use of PhotoDNA, Chatstep identified two images allegedly distributed by Rosenschein as child pornography before the images were submitted to the NCMEC. NCMEC did not view the images, but determined the probable physical origin of the images, and forwarded the material to the New Mexico Attorney General's Office Internet Crimes Against Children Task Force. This prosecution followed.

Rosenschein issued a subpoena under the authority of Fed. R. Crim. P. 17 to Microsoft on October 11, 2018, [Doc. 125-1, p. 6], requesting the following documents:

- a. Any and all agreements, formal or informal, memoranda of understanding, directives, guidelines, correspondence, policies, procedures, or other documentation concerning cooperation between Microsoft and law enforcement agencies, including, but not limited to, law enforcement agencies in the State of New Mexico (including the New Mexico Attorney General's Office) or the National Center for Missing & Exploited Children ("NCMEC"), addressing Microsoft's PhotoDNA program, the sharing of hash values related to the PhotoDNA program, or maintaining any set of hash values associated with apparent or actual child pornography to be used with the PhotoDNA program.
- b. Copies of any and all documents, electronic correspondence, or other communications sent by Microsoft and/or Microsoft's PhotoDNA program or API associated with the Photo DNA program to NCMEC on behalf of any Chatstep.com user with the moniker "Carlo" on or about July 25, 2016 through August 10, 2016, concerning those matters addressed in the July 31, 2016 CyberTipline Report 13456293 (Exhibit A) and August 8, 2016 CyberTipline Report 13596645 (Exhibit B), including copies of any electronic data, notices or reports that Microsoft's photoDNA program or associated API reported to NCMEC (excluding any files containing any photographic images).

- c. The URL of any website used by the Microsoft PhotoDNA service that provided NCMEC with the cyber tip information related to Chatstep.com user "Carlo" as referenced above in section (b).
- d. The IP address and/or email address used by the Microsoft PhotoDNA program or associated API from which any data, cyber tips, notices or other reports referenced above in section (b) originated.
- e. Identification of the individual employed by either Microsoft or Chatstep who was responsible for forwarding any data, notices or other reports referenced in section (b), including name, last known address, phone number and email address, if known. If the reporting individual was not a person, identify the computer program or algorithm that forwarded the data or report to NCMEC.
- f. Copies of any and all guidelines, memoranda of understanding policies, procedures or other documentation related to the Microsoft PhotoDNA program, in particular any memorandums of understanding or terms of service that were used by Microsoft or posted on the PhotoDNA Internet page during the months of July and August of 2016. This request includes all such materials that were in place with Chatstep.com and NCMEC during July and August of 2016.
- g. Copies of any memorandums of understanding, contracts, terms of service, agreements or correspondence (in any medium, including email, texts, chats, or other oral or written communications) that Microsoft or any of its subdivisions or subsidiaries has or had with Chatstep or NCMEC addressing Microsoft's Photo DNA program, including, but not limited to, agreements for providing any data, CyberTipline reports, notices, or the use of other shared information like hash value sets. This request includes all documents and material addressing how Microsoft's PhotoDNA program would interact with Chatstep.com to search files posted by Chatstep.com's users then provide any data or CyberTipline reports to NCMEC, especially the two CyberTipline reports addressed in paragraph c above.
- h. All correspondence in any form (U.S. mail, private courier, email, texts, chats, telephone logs, telephone notes etc.) that Microsoft sent to or received from the developers or owners of the domain name "Chatstep.com" to either the email address devs@chatstep.com, the street addresses 10190-1 Pasadena Ave., Cupertino, California 95014, or 10012 Byrne Ave, Cupertino, California, 95014, or any other destination or email related to Chatstep, addressing or touching upon how to apply for the PhotoDNA program, why Chatstep was initially rejected by Microsoft, how to interface the Photo DNA reporting program with NCMEC, troubleshooting the operation of the Photo DNA reporting program with either Microsoft or NCMEC, ensuring that the reports that PhotoDNA program (or the API associated with that program) were making on behalf of Chatstep were operating correctly. This request includes email attachments or documents referred to in any of these communications.

- i. All correspondence in any form (U.S. mail, private courier, email, texts, chats, telephone logs, telephone notes, CyberTipline Reports, data transmissions, etc.) that Microsoft sent to or received concerning the July 31, 2016 CyberTipline Report No. 13456293 or the August 8, 2016 CyberTipline Report No. 13596645, including but not limited to the URL or IP address of each sender or recipient involved with each electronic correspondence or data transfer.
- j. Microsoft.com's registration materials or documents detailing Microsoft.com's (or any Microsoft's subsidiary, including the subsidiaries that control the Digital Crimes Unit or PhotoDNA) registration with NCMEC's CyberTipline, and confirmation that the appropriate sign in credentials were assigned to Microsoft.com.
- k. All of Microsoft's Memorandum of Understandings or similar contractual agreements with NCMEC or any other entity addressing the sharing of any set of hash values associated with apparent child pornography images or videos, including but not limited to the Industry Hash Sharing Platform, the Industry Hash Sharing Database, the Technology Coalition hash set, NCMEC's hash database or list, or any set of hash values originating from any Canadian government or organization.
- l. Any documentation concerning the hash value match associated with either the July 31, 2016 CyberTipline Report No. 13456293 or the August 8, 2016 CyberTipline Report No. 13596645, including the identifying name of the hash value set used by the PhotoDNA program that matched the purported upload of an image with any value contained in a hash value set and the actual hash value and hash match number.
- m. All reports or correspondence in any form or medium either sent to or received from any source or entity whatsoever concerning the PhotoDNA report on behalf of Chatstep.com that resulted in the July 31, 2016 CyberTipline Report No. 13456293 or the August 8, 2016 CyberTipline Report No. 13596645, including the IP address or URL for everyone involved in each communication, especially the IP address or URL of the entity sending the original report to NCMEC alerting NCMEC to these two reports. This request includes the original data transfer from Microsoft's PhotoDNA API reporting program to NCMEC concerning these two CyberTipline reports, and all of the data fields that Microsoft's reporting API for the PhotoDNA program populated or left blank associated with those two reports, as well as all documentation addressing how NCMEC received these two reports or followed up on these reports.
- n. Any document, correspondence or communication in any form or medium addressing any assistance that Microsoft (including the Digital Crimes Unit of Microsoft) offered or provided to NCMEC touching upon NCMEC's presentation at the Crimes Against Children Conference for 2017 entitled as follows:

## Emerging Issues and Insights Related to Child Pornography Cases Based on CyberTipline Reports

*Yiota Souras, Rebecca Sternburg*

To date, the National Center for Missing & Exploited Children has received over 17 million reports relating to child sexual exploitation images and videos submitted by the public and electronic service providers to NCMEC's CyberTipline. Building on years of experience assisting with thousands of reports, join staff from our Office of Legal Counsel and from our Exploited Children Division team for an in-depth look at the CyberTipline. Topics will include: how reports are received and processed, the holding in *U.S. vs. Ackerman* and specific challenges to anticipate and address in the aftermath of this decision, and free legal resources and technical assistance available from NCMEC.

### **Target Audience:** LE, Pros

- o. All correspondence between Microsoft and NCMEC addressing NCMEC's PhotoDNA Initiative, the program that NCMEC supported so that electronic service providers on the Internet could use Microsoft's PhotoDNA program. The PhotoDNA Initiative at issue here is the one discussed on the Technology Coalition's web page at [ww.techologycoalition.org/coalitionprojects/](http://ww.techologycoalition.org/coalitionprojects/). (Last visited on May 27, 2018).
- p. All correspondence or documentation, including memorandums of understanding or terms of use, between Microsoft and NCMEC touching upon NCMEC's PhotoDNA Initiative discussed in paragraph s.
- q. All correspondence between Microsoft and NCMEC addressing NCMEC's ability to use the PhotoDNA program or to sublicense the PhotoDNA program and related technology to third parties.
- r. All correspondence with any law enforcement agency or officer (which includes NCMEC) concerning the PhotoDNA report that resulted in NCMEC's July 31, 2016 CyberTipline Report No. 13456293, or NCMEC's August 8, 2016 CyberTipline Report No. 13596645.

[Doc. 125-1, pp. 9-12 (bold type in original)].

The parties met and conferred in an attempt to narrow these requests, but were ultimately unsuccessful. [See Doc. 125, pp. 4-8; Doc. 136, pp. 7-8]. Microsoft then filed this Motion, asking the Court to modify the subpoena. Microsoft argues that the subpoena fails to satisfy the Rule 17(c) requirements of specificity, relevancy, and admissibility. [See Doc. 125, pp. 8-14]. Alternatively,

Microsoft argues that the burden imposed by the subpoena is unreasonable and oppressive, [*see id.*, pp. 14-17], predicting “based on its experience with past document production ... it would cost the company more than \$1 million to host and review the documents.” [*Id.*, p. 15; *see also* Doc. 125-2, p. 2]. Microsoft also argues that compliance with the subpoena would result in the production of documents relating to the technical engineering of PhotoDNA, and require it to review the documents for proprietary, commercially sensitive, and privileged information. [*Id.*]. Microsoft asks for an order which would limit its duty to search to the following categories of documents:

- Agreements pertaining to PhotoDNA between Microsoft and any federal law enforcement agency or State Attorney General;
- Agreements between Microsoft and third parties regarding hash sharing;
- Information regarding the specific CyberTipline Reports in this case, dated July 31, 2016, and August 8, 2016;
- Guidelines, memorandums of understanding, policies, procedures, or Terms of Service that were applicable to the Microsoft/Chatstep or Microsoft/NCMEC relationship in July or August 2016;
- With respect to email correspondence, only those emails exchanged between Microsoft and Chatstep regarding Chatstep’s use of the PhotoDNA Cloud Service, including any correspondence regarding how Chatstep came to locate Microsoft’s PhotoDNA Cloud Service.

[Doc. 125, pp. 17-18].

Rosenschein responds that his subpoena is reasonable because “documents concerning collaboration of Microsoft and NCMEC concerning the development of PhotoDNA are material

to the agency relationship between Microsoft and NCMEC.” [Doc. 136, p. 12]. Rosenschein explains that he intends to prove that Microsoft was acting as an agent of the government “through developing PhotoDNA with NCMEC as well as supporting NCMEC and participating in the PhotoDNA Initiative[.]” [*Id.*]. He argues that he “must have access to the materials and documentation that reflect the relationship of Microsoft to law enforcement entities, including NCMEC, as well as the knowledge and acquiescence of law enforcement agencies, like NCMEC, to allow Microsoft to serve their interests.” [*Id.*]. Rosenschein concludes that the materials described in the subpoena categories are admissible and relevant, [*id.*, p. 16], and, as narrowed by his February 18, 2019, proposal to Microsoft, sufficiently specific. [*See id.*, pp. 17-21]. He observes that his requests, as modified, “are self-limiting in time as they either refer to the specific CyberTips at issues (sic) in this case, or simply the life of the PhotoDNA program which is from 2008 to present.” [*Id.*, p. 21]. “Microsoft is the most valuable company in the world,” according to Rosenschein, and “has not demonstrated that the costs of compliance are unduly onerous in light of the financial holdings of the Corporation, nor have they attempted to associate the cost of compliance with the narrow terms that were proposed by Dr. Rosenschein on February 18, 2019.” [*Id.*, pp. 22-23].

Microsoft replies that, in this Circuit, “a Rule 17(c) subpoena must be quashed or modified if the proponent cannot ‘identify the item sought and what the item contains.’” [Doc. 138, p. 6 (quoting *United States v. Morris*, 287 F.3d 985, 991 (10th Cir. 2002))]. Therefore, Microsoft submits Rosenschein’s requests fail Rule 17(c)’s specificity requirement even as modified by his proposal. [*Id.*]. Microsoft maintains that “even setting aside the requests Defendant fails to defend, his subpoena remains unreasonable and oppressive[.]” [*id.*, pp. 10-11], because compliance, even as modified by Rosenschein’s proposal, would cost it hundreds of thousands of dollars. [*Id.*].



### III. LEGAL STANDARDS

Federal Rule of Criminal Procedure 17(c) authorizes pretrial subpoenas *duces tecum* in criminal cases for limited purposes. Rule 17(c) was never intended to be a tool for discovery. *See Nixon*, 418 U.S. at 698. Thus,

[a] party seeking a subpoena *duces tecum* pursuant to Rule 17(c) must show: (1) that the documents are evidentiary and relevant; (2) that they are not otherwise procurable reasonably in advance of trial by exercise of due diligence; (3) that the party cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection may tend unreasonably to delay the trial; and (4) that the application is made in good faith and is not intended as a general “fishing expedition.”

*Morris*, 287 F.3d at 991 (quoting *Nixon*, 418 U.S. at 699-700). In order to meet its burden, the proponent of a subpoena “must clear three hurdles: (1) relevancy; (2) admissibility; and (3) specificity.” *Id.* Failure to clear even one of these hurdles will result in the modification of the subpoena. *See United States v. Abdush-Shakur*, 465 F.3d 458, 467 (10th Cir. 2006).

“Specificity is the most difficult hurdle to overcome.” *United States v. Wittig*, 247 F.R.D. 661, 663 (D. Kan. 2008) (citation omitted). “*Nixon*[’s specificity requirement] mandates that the party requesting the information identify the item sought and what the item contains, among other things.” *Morris*, 287 F.3d at 991. Thus, “[t]he specificity requirement ensures that Rule 17(c) subpoenas are used only to secure for trial certain documents or sharply defined groups of documents.” *Wittig*, 247 F.R.D. at 663.

For example, the special prosecutor who issued the subpoena in *Nixon* was able to identify the participants and time and place of the sought-for taped conversations, and so the subpoenas were upheld by the Court. *See Nixon*, 418 U.S. at 700. In contrast, the Tenth Circuit in *Morris* held that a subpoena was properly quashed for lack of specificity where it sought all documents surrounding an FBI agent’s shooting of the defendant as well as the agent’s personnel file. *Morris*,

287 F.3d at 991. Prior to *Morris*, the Tenth Circuit held a subpoena to be overbroad where it requested evidence to show that the arresting officer had a propensity to make pretextual stops and to impeach his credibility. *See United States v. Hughes*, 931 F.2d 63 (10th Cir. 1991) (unpublished). In sum, “a Rule 17 subpoena *duces tecum* cannot substitute for the limited discovery otherwise permitted in criminal cases and the hope of obtaining favorable evidence does not justify the issuance of such a subpoena.” *Richardson*, 607 F.3d at 368-369; *see also Stevenson*, 727 F.3d at 831 (“The relevance and specificity elements require more than the title of a document and conjecture as to its contents, and a subpoena should not issue based upon a party’s mere hope that it will turn up favorable evidence.”).<sup>1</sup>

#### IV. ANALYSIS

##### **A) The Court should modify Rosenschein’s subpoena because the requests it contains are not sufficiently specific.**

As noted, failure of the proponent of a subpoena to clear even one of the *Nixon* hurdles permits modification of the subpoena. Even assuming if Rosenschein can demonstrate the relevance and admissibility of the categories of documents he seeks, he has failed to identify those documents with the required specificity. The majority of his requests (a, b, f, g, h, i, k, l, m, n, o, p, q, and r), seek “any and all” or “any” documents related to Microsoft’s relationships with law enforcement and Chatstep and are clearly aimed at discovering documents that Defendant Rosenschein does not presently know exist. *See Wittig*, 247 F.R.D. at 664 (“Defendant’s proposed subpoenas clearly resemble discovery requests, employing such terms as ‘any and all’ documents or communications, or ‘includes, without limitation.’”). Only after the parties met and conferred

---

<sup>1</sup> In arguing to the contrary, Defendant Rosenschein urges the Court to adopt the standard employed in *United States v. Nosal*, 293 F.R.D. 403, 409 (N.D. Cal. Mar. 1, 2013), which concluded that requests in a Rule 17(c) subpoena need only be “material to the defense” and “not overly oppressive.” [See Doc. 136, pp. 10-11, 17]. The Court rejects this articulation as contrary to the *Nixon* standard and for the reasons stated in Microsoft’s Reply brief (i.e., that it is by far the minority view, and was even set aside by the district judge presiding over *Nosal*). [See Doc. 138, p.5].

were these topics narrowed to be “self-limiting in time as they either refer to the specific CyberTips at issues (sic) in this case, or simply the life of the PhotoDNA program which is from 2008 to present.” [Doc. 136, p. 21]. Even as narrowed, however, the Court finds that these requests run afoul of *Nixon*’s specificity requirement.

The Court takes guidance from analogous decisions of the Fourth and Eighth Circuits in *Richardson*, 607 F.3d at 368-369, and *Stevenson*, 727 F.3d at 831. In both, the defendant sought to develop an agency argument between the government and an internet service provider in a child pornography prosecution, but the district courts quashed the subpoenas, finding that they failed *Nixon*’s requirements. On appeal, the Fourth and Eighth circuits each affirmed because the document requests issued by the defendants, though relevant, were too vague, suggesting instead attempts at exploratory discovery. So too here.

Even Rosenschein’s requests that are arguably narrow (c, d, e, and j), still verge on exploratory discovery. For example, in request c, Rosenschein is unable to identify the website used to provide information to NCMEC concerning the two Cybertips in this case and asks Microsoft to provide this information. [See Doc. 136, p. 18]. The same is true for the IP addresses at issue in request d, and the names of the Chatstep or Microsoft employees responsible for forwarding the information concerning the two Cybertips in request e. [See *id.*]. Finally, request j seeks “Microsoft.com’s registration materials or documents detailing Microsoft.com’s ... registration with NCMEC’s CyberTipline, and confirmation that the appropriate sign in credentials were assigned to Microsoft.com,” not identifying specific documents Rosenschein needs to prove his agency argument.

Microsoft is agreeable, however, to providing more than the Court would otherwise require. Therefore, the Court will honor Microsoft’s commitment to provide agreements pertaining

to PhotoDNA and any federal law enforcement agency or State Attorney General, and agreements with third parties regarding hash sharing. [See Doc. 126-1, p. 1]. It has also agreed to provide information regarding and relevant to the Cybertipline Reports in this case, as well as the guidelines, memorandums of understanding, policies, procedures, or terms of service that were applicable to its relationships with Chatstep and NCMEC. [*Id.*]. Microsoft has further agreed to provide emails pertaining to Chatstep's use and discovery of the PhotoDNA Cloud Service. [*Id.*, p. 2]. The Court finds that these stipulations are reasonable and reflect the parties' agreement.

**B) Alternatively, the Court should modify Rosenschein's subpoena as issued because it is oppressive.**

Microsoft has presented evidence that compliance with the subpoena as issued would cost more than one million dollars. [Doc. 125-2, p. 2]. While Microsoft may be a company of nearly endless resources, [see Doc. 136, p. 22], such a burden on a non-party is disproportional to a case such as this. If every defendant in every child pornography prosecution were to be permitted to make such requests service providers would be forced to abandon preventative efforts.

The cases Rosenschein cites do not convince the Court otherwise. The court in *In re August, 1993 Regular Grand Jury (Med. Corp. Subpoena II)*, 854 F. Supp. 1392, 1402 (S.D. Ind. 1993), was addressing a grand jury subpoena issued to a potential defendant corporation, not a pretrial subpoena issued to a third party. The same is true of *Matter of Midland Asphalt Corp.*, 616 F. Supp. 223, 225 (W.D.N.Y. 1985). In sum, the Court is not convinced that Microsoft should be required to shoulder the burden of complying with the subpoena as drafted.

**C) Defendant Rosenschein's Request for a Hearing Should be Denied.**

In moving for a telephonic hearing before this Court, Rosenschein described his Rule 17(c) Subpoena to Microsoft as "essential" to his motions to suppress, then scheduled to be heard during the week of June 10, 2019. [Doc. 141, p. 1]. Rosenschein went on to explain that "Microsoft's

Reply raised issues that require clarification regarding Dr. Rosenschein's defense of his Rule 17(c) subpoena requests as narrow (sic) in the Response" and that, "[i]n lieu of requesting leave to file a surreply, defense counsel can address these issues at a hearing before the Court." [*Id.*, p. 2]. Rosenschein did not elaborate as to which issues require clarification. [*Id.*]. Instead, he contemporaneously moved to continue the June 10, 2019, suppression hearing [*see* Doc. 145], never thereafter moving the Court for leave to file a surreply. Microsoft takes the position that the Motion can and should be decided on the briefs. [Doc. 141, p. 1].

Rosenschein has not cited to, and the Court is not aware of, any rule of procedure nor case that requires a hearing in these circumstances, and Rosenschein has not identified any factual dispute that needs to be explored. The Court finds that the legal issues pertaining to whether Microsoft's Motion to Modify should be granted can be determined on the briefs. Therefore, the Court recommends that Rosenschein's request for a hearing be denied.

## **V. CONCLUSION**


Above all, "Rule 17(c) was not intended to provide an additional means of discovery." *Bowman Dairy Co.*, 341 U.S. at 220. For this reason, the proponent of a subpoena must know what he is requesting and be able to specify its contents. Rosenschein's subpoena in this case did not conform to this requirement.

Wherefore, IT IS HEREBY RECOMMENDED Non-Party Microsoft Corporation's Motion to Modify Rule 17(c) Subpoena [Doc. 125], be **granted** and that Defendant Rosenschein's Request for a Telephonic Hearing on the Motion be **denied**. IT IS FURTHER RECOMMENDED that the Court enter an Order requiring Microsoft to produce the following specific categories of documents, but no others:

- Agreements pertaining to PhotoDNA between Microsoft and any federal law enforcement agency or State Attorney General;
- Agreements between Microsoft and third parties regarding hash sharing;
- Information regarding the specific CyberTipline Reports in this case, dated July 31, 2016, and August 8, 2016;
- Guidelines, memorandums of understanding, policies, procedures, or Terms of Service that were applicable to the Microsoft/Chatstep or Microsoft/NCMEC relationship in July or August 2016;
- With respect to email correspondence, only those emails exchanged between Microsoft and Chatstep regarding Chatstep's use of the PhotoDNA Cloud Service, including any correspondence regarding how Chatstep came to locate Microsoft's PhotoDNA Cloud Service.

[See Doc. 125, pp. 17-18].

SO ORDERED.



---

Jerry H. Ritter  
U.S. Magistrate Judge

**THE PARTIES ARE FURTHER NOTIFIED THAT WITHIN 14 DAYS OF SERVICE** of a copy of these Proposed Findings and Recommended Disposition, they may file written objections with the Clerk of the District Court pursuant to 28 U.S.C. § 636(b)(1).

**A party must file any objections with the Clerk of the District Court within the fourteen-day period if that party wants to have appellate review of the proposed findings and recommended disposition. If no objections are filed, no appellate review will be allowed.**